NEW YORK TIMES
26 June 1985

U.S. to Replace Many Embassies And Consulates for Better Security

By JOEL BRINKLEY
Special to The New York Times

WASHINGTON, June 25 — The State Department has decided to renovate or replace almost half of its 262 embassies and consulates around the world because the existing buildings are vulnerable to espionage or terrorist attack, department officials said today.

In what would be the most ambitious building and security program in the department's history, over the next seven years 75 embassies and consulates worldwide will be abandoned and then rebuilt at new locations, according to Robert E. Lamb, Assistant Secretary of State for Administration.

Another 50 will be substantially renovated or rebuilt on site. In addition, 210 foreign offices of the United States Information Agency, Foreign Commerical Services and the Agency for International Development will be renovated or replaced, too. The cost of all this work, Mr. Lamb said, will be at least $3.5 billion.

State Department officials would not identify the embassies and consulates involved because they did not want to tell terrorists which were vulnerable, an official said.

Eight-Member Panel

The building program and other measures are in response to recommendations from a special State Department Advisory Panel on Overseas Security, whose report was issued today.

The eight-member group, appointed by Secretary of State George P. Shultz last July and headed by Adm. Bobby R. Inman, former Deputy Director of Central Intelligence, was highly critical of the State Department's foreign security programs.

The report said security programs overseas were disorganized and confused, adding that security offices were "grossly understaffed" and poorly trained.

Foreign nationals hired as guards at some posts around the world were illiterate or incompetent, the panel found, and the responsibility for embassy security was divided among so many different people and offices that different security "survey teams visiting posts abroad often make contradictory recommendations," the report said.

Endorsement of Findings

Mr. Lamb said Secretary of State George P. Shultz had endorsed the panel's findings in principle, and he "asked that we proceed quickly to implement the recommendations."

Among the other panel members were Lawrence S. Eagleburger, former Under Secretary of State, and Anne L. Armstrong, former Ambassador to Great Britain and now chairman of the President's Foreign Intelligence Advisory Board.

Mr. Lamb said the group's findings surprised the State Department. "We knew we had a problem," he said, "but we didn't expect it to be of this magnitude."

Although officials would not identify the 126 embassies and consulates to be renovated or replaced, Mr. Lamb said most of them "are former residences or offices that we have been putting layer after layer of security on" over the last few years.

Many of them are so close to the street that they cannot be effectively protected against vehicle bombs, he said. The car bombings of two embassies in Lebanon and one in Kuwait over the last two years, killing almost 100 people overall, were the major impetus for the report and the rebuilding program.

Other embassies and consulates, including almost every one in Soviet bloc countries, adjoin other buildings, making it difficult to protect them from electronic listening devices, officials said. Mr. Lamb said a principal reason for the new building program was that, "We are facing a very serious espionage threat from electronic and other means."

Mr. Lamb said the department has not decided how it will pay for the building program, although he said the $3.5 billion expense will be spread over at least five budget years. All the new embassies should be complete in about eight years, he said.

The panel also recommended that the State Department convene a formal board of inquiry "with the powers of establishing accountability in all cases involving terrorism or security-related attacks." Members of Congress and others have criticized the State Department for failing to assign responsibility following past terrorist attacks that appeared to be the result of inadequate security.

Mr. Shultz has accepted that recommendation, the report said. Mr. Lamb said the purpose of the boards of inquiry would "not be to find someone to punish," although he added that "it may very well be that people will be fired" or disciplined as a result of any future board of inquiry investigations.

Mr. Lamb said he will leave his present job next week to begin putting the report's more than 90 recommendations into effect. Other suggestions deal with staffing, bureaucratic organization, training of personnel and intelligence matters, among others.

ARTICLE APPEARED
ON PAGE A3

NEW YORK TIMES
25 June 1985

Embassy in Soviet to Drop Russians

By JOEL BRINKLEY
Special to The New York Times

WASHINGTON, June 24 — The State Department plans to reduce the number of foreign nationals working in American embassies in Soviet-bloc countries because many of them are believed to be spies, Government officials said today.

Meanwhile, Secretary of State George P. Shultz told a Senator that he "endorsed in principle" an advisory panel's recommendation that dozens of new embassies and consulates be built around the world to discourage terrorist attacks.

In a letter to Senator Richard G. Lugar, the Indiana Republican who is chairman of the Foreign Relations Committee, Mr. Shultz said the cost of construction had been put at more than $3 billion dollars over the next five to seven years.

The reduction of foreign employees and the construction program are among actions recommended in a report by an Advisory Panel on Overseas Security that Mr. Shultz set up in July 1984. The panel was headed by Adm. Bobby R. Inman, former Deputy Director of Central Intelligence.

Secret Portion Is Described

An expurgated version of the report describing the building proposal is to be made public Tuesday, but a summary was made available today. A 50-page supplement detailing espionage problems in United States embassies in Soviet-bloc countries wil not be made public, but Government officials and members of Congress described its contents today.

According to Senator Patrick J. Leahy, a Vermont Democrat who as vice chairman of the Senate Select Commitee on Intelligence has been briefed on the problem, the report says so many Russians, including known intelligence agents, are employed at the American Embassy in Moscow that the embassy "is a sieve."

About half of the nearly 400 people working in the embassy in Moscow are Soviet citizens. The ratio of foreign nationals to United States citizens is similar in other embassies in Soviet-bloc capitals, just as it is in most other American embassies around the world.

But in Soviet-bloc capitals, officials said, local citizens can generally work in Western embassies only with the approval of their governments, which usually means security clearance and approval of the security agencies of the host countries.

"Sure there are agents of the K.G.B." a State Department official said today, referring to the Soviet internal security and intelligence agency, "but there are also many loyal employees who have worked for us for years despite great hardships."

The Soviet citizens are employed in such jobs as secretaries, photocopiers, chauffeurs, repairmen and groundskeepers.

Practice Has Long Been Debated

Members of Congress and State Department officials have long debated the wisdom of employing Soviet citizens. The State Department has defended the practice, on the ground that Soviet citizens have no access to American secrets.

But, according to an intelligence official, the advisory panel found that Soviet citizens are "so pervasive throughout the embassy" that by watching and reading available materials they can gather sensitive information.

The State Department has insisted that there have been no major security breaches. But early this year officials acknowledged that electronic bugging devices had been found in embassy typewriters.

A Soviet employee had been in charge of assigning typewriters, and when the devices were discovered, one typewriter was being used by the secretary of the deputy chief of mission, the embassy's second ranking officer, an intelligence official said today.

Officials who have read the advisory report said that it described several other instances of security breaches attributed to Soviet employees.

The officials said that listening devices had been found in some embassy vehicles and that Soviet employees might have typed early versions of documents that were later classified as confidential or secret. Although the early versions probably did not contain sensitive material, the officials said, the Soviet employees could obtain useful information by reading the initial material, overhearing conversations and then watching the comings and goings of embassy personnel.

State Dept. Opposes Limitations

The State Department has resisted replacing the Soviet employees because of the cost of hiring, training and housing hundreds of Americans for menial jobs in Moscow and other Soviet-bloc capitals. In addition, a State Department official said, "these are the people who actually live in the society and can get things done for us."

The State Department has opposed legislation that would limit the number of local employees in Soviet-bloc countries to the number of Americans employed by the embassies of the host countries in Washington. The Soviet Embassy here has fewer than 10 American employees, Senator Leahy said, a sponsor of the legislation.

The legislation has passed the Senate and will be discussed in a Senate-House conference. A State Department official said, "We don't think we should be dictated to on this question."

But several officials said the Administration had decided, partly in reaction to the advisory report, to reduce the number of foreign employees in Soviet-bloc counries.

The espionage problem is also a reason behind the proposal to build new embassies and consulates. In Soviet-bloc countries, officials said, host governments can plant listening devices in embassy walls. But the principal reason for the building proposal is the threat of terrorism in countries outside the Soviet bloc.

ARTICLE APPEARED ON PAGE 25

TIME
17 June 1985

Nation

Moles Who Burrow for Microchips

How high tech has raised the stakes of Soviet espionage in the U.S.

Were it not for a few telltale antennas and a curious whitewashed rooftop coop, the handsome brick edifice in San Francisco's tony Pacific Heights could be easily mistaken for a small, posh hotel. In fact, the owner is the Soviet Union and the occupants are at least 41 Soviet officials. That is an unusually large number of diplomats for a consulate in a medium-size American city, but the Soviets did not come to the Bay Area to stamp tourist visas. About half the consular officials, the FBI estimates, are actually spies.

The Soviets bought the building for its sweeping vistas of the bay, as well as its unobstructed microwave reception. The electronic gadgetry on the roof scans the airwaves and can pluck out conversations when a computer recognizes certain words or phrases. On a clear day, the Soviets can watch Navy aircraft carriers cruising under the Golden Gate Bridge and jets taking off from the Alameda Naval Air Station to the east. But the activity that truly intrigues the Soviets is 40 miles to the south, in Silicon Valley.

There, amid the taco joints and shopping malls, are hundreds of burgeoning high-tech firms that help give the U.S. its essential—but fast shrinking—edge over the Soviets in high-technology equipment. From their high-rent spy nest in San Francisco, KGB agents fan out through the valley, looking for Americans who can be bought and secrets that can be stolen.

Moscow's hunger for high tech has transformed the ancient art of spying. No longer are the Soviets principally interested in the traditional fruits of espionage—the enemy's order of battle, troop movements and codes—even though, as the Walker case vividly demonstrates, they would dearly like to know the secrets of U.S. antisubmarine warfare. High tech has both raised the stakes and broadened the game. It has made the Silicon Valley microchips as valuable as NATO war plans, and it has made traitors out of civilian engineers as well as Navy code clerks.

Kremlin scientists cannot possibly compete with their U.S. counterparts in the race of microchips and laser beams that have increasingly become the sinews of modern warfare. The Soviets have long been able to build powerful rockets and sturdy tanks, but their home-designed computers are slow and crude. To close the gap, the Soviets have waged a massive and successful campaign to capture America's technological wizardry. Since the late '70s, estimate U.S. intelligence experts, the Soviets have made off with 30,000 pieces of high-tech equipment and 400,000 technical documents. As a result, declares Assistant Secretary of Defense Richard Perle, they have cut the U.S. technological lead from ten years to as little as three. For the U.S. and its NATO allies, who rely on brains to beat brawn, on "smart weapons" to counter the larger Warsaw Pact forces, the high-tech drain is a factor of consequence in the precarious balance of power.

JIM POLLARD

Customs agents inspecting export-bound circuit boards

KGB spies are held to quotas just like salesmen.

The Reagan Administration has tried to limit the sale of high-tech equipment that can be put to military use and to crack down on the international "technobandits" who purchase or steal for the Soviets what they cannot directly buy. But in an open society that must trade freely with the world, the Reaganauts have about as much chance of preventing high-tech secrets from flowing out of the U.S. as they do of stopping cocaine and marijuana from flooding in.

Stealing high-tech secrets is nothing new; the Soviets have been doing it since at least the 1930s, when Communist agents made off with Western inventions like Eastman Kodak's formula for developing color pictures. In the late '40s the Russians even managed to steal atomic secrets. But in the 1960s, as the U.S. outmatched the Kremlin's big missiles with more accurate ones, Soviet spies were ordered by their masters to make high tech their No. 1 target. It is U.S. computer technology that the Soviets truly covet, for the ability to process masses of information in milliseconds is what makes modern weapons so deadly. Says FBI Counterintelligence Chief Ed O'Malley: "Science and technology is the KGB's largest growth industry."

Détente, with its scientific exchanges and increased East-West trade, was an enormous windfall for the Soviets. Pentagon officials still shake their heads over the guile of Soviet engineers who, as they toured a U.S. aircraft factory during the 1970s, would wear sticky-soled shoes to pick up metal filings. When the U.S. sent young scholars to Moscow to study Slavic languages, the Soviets exchanged "graduate students" who were often middle-age technocrats with a more than academic interest in microcircuitry. A huge truck factory built in the Soviet Kama region with U.S. financing and know-how, all acquired aboveboard, was put to work making the army transports that now convoy Soviet troops over the Afghanistan countryside. Far worse, grinding machines that can craft tiny ball-bearings, legally sold to the Soviets by a small Vermont company in 1972, have in the estimate of U.S. intelligence experts saved the Soviets about a decade of R. and D. on improving the accuracy of their ICBMs.

Today many Soviet weapons are reasonable facsimiles if not exact duplicates of American ones. The Soviet AWACS and space shuttles are carbon copies of earlier U.S. models. The Boeing short takeoff and landing (STOL) prototype, a breakthrough aerodynamic design, miraculously appeared just 16 months later as the Soviet AN-72. The SU-15 fighter that shot down the Korean Air Line's Flight 007 two years ago did so with a missile guidance system designed in the U.S. The Soviets do not even attempt to create their own computers anymore: the Kremlin's mainframe RIAD computer is IBM's 360 and 370 series of mainframes, right down to the color of its wires, while the Soviet AGAT personal computer is a copy of the Apple II.

The Soviets decide what to buy or steal by wading through the flood of technical journals and documents freely available in the U.S. Specialized translators at

ARTICLE APPEARED
ON PAGE A-13

WASHINGTON POST
10 June 1985

Bobby R. Inman

The Walker Case: A Direct Hit?

The former deputy director of Central Intelligence is interviewed by Stephen S. Rosenfeld.

Q: What's the value of the loss to our security in the Walker spy case?

A: All we know really is where the people served. If you look at their duty stations, there are some judgments that you can make about worst-case kind of losses. First . . . would be service on an SSBN, a U.S. ballistic missile submarine; that would have been at or near the top of Soviet interests. How the SSBN operated, where, when did it come near the surface to communicate, did it transmit communications, if so, exactly what time, when, where, on what frequencies?

A good deal of that fortunately has been ameliorated by time. And because of the advent of Trident, we're operating in entirely different areas—different missile systems, a great many things are different. While the damage could have been very severe at the time, the prospect of its being useful still to increase the vulnerability of that part of our deterrent force has been substantially reduced.

The second major area of possible loss would be from the service [by one of the suspects] with attack submarines—the ability to see the communications from the attack submarines. Revealing details on how we went about detecting Soviet units, the effectiveness of it, how we operated, what kinds of tactics we used, what kinds of tactics we might use if we were to move into a time of crisis or hostilities. There could have been insights into our other means of locating foreign submarines, including some impact on both surface and air capability. And there, because systems stay in place a lot longer, the damage could be enduring.

The third area that is still pretty murky is the degree of exposure to surface, amphibious and naval air warfare areas, where there is the potential that message traffic could have been provided on the details of exercises, exercising our war plans, candid assessments of weaknesses of equipment or of tactics and doctrine. All those that have proven particularly valuable.

The fourth area would have to do with the security of communications. Here, because of losses in the '50s, early '60s, the U.S. has moved to vastly more expensive and complex means of protecting its own communications. Variable, changing, keying material every day, designed to withstand the damage from an occasional individual who would sell a code of security.

I inherently worry when I see that one of these indivduals was a crypto repairman, and the prospect that they were in position to provide materials for years. Even the best of systems could come under some attack under those circumstances.

Now, that's clearly a worst-case look. It would require a continuous flow of material for a very long time, and we do not in fact know at this point in time that that did occur.

Q: In the spectrum of cases over a period of time, this is one of the worst?

A: It would not reach the magnitude in my judgment of the Klaus Fuchs-Rosenberg passing-over of nuclear weapons. But it sure stands pretty high on the list of those that come thereafter—in prospective damage. It may turn out, if we're lucky, that there was substantially less than could have occurred.

Q: How could this have happened? What produced this hemorrhage, and why wasn't it caught in time?

A: We know that during the '70s there was strong bipartisan support to try to improve trade and long-term relationships, and we permitted a substantial increase in the number of Soviet citizens in this country legally and East Europeans and the PRC, other nations as well. In the same time frame, we were drawing down resources across the national security account and elsewhere in government, and the number of counterintelligence agents in the FBI and the military services were drawn down substantially. So there was a mismatch in the numbers of people trying to maintain continuous surveillance of those who could be engaged in recruiting and running spies.

Then, there has been an increase in the total numbers of people with access to classified information, and there have been allegations—probably reality from time of time—of information being classified that didn't merit classification.

Finally, beginning in the middle '60s, there was a substantial hemorrhage of classified information being leaked to the press. Newsmen didn't go into the offices and take classified documents off desks. They were given them by government employees authorized to have access to classified information. There was an impact on the judgment of individuals about the value of the information they were charged to protect.

If you've got a young enlisted man who's already got a family who's living close to the poverty line, he sees a classified message, he looks at the front page of a newspaper and sees the same information, he knows that someone provided that. And if he's been approached, the temptation is to go ahead—since there's already been a damage—to sell the information for cash. Certainly all this increased the hazard that people would elect to sell.

In looking at the personnel security system, you've got different categories of information to protect. You've got, we're told in recently published figures, perhaps 100,000 people with the most sensitive level of clearance. Those people are subjected to very detailed background investigations every five years. A substantial percentage—civilians at the National Security Agency, all employees of the Central Intelligence Agency—are subject to polygraph examinations as a part of that process.

Continued

The next largest category, 600,000 or so, the figures indicate, have access to top secret including cryptographic materials. There again, background investigations are conducted—polygraphs are not used—and they are less rigorous than those for the most sensitive level of clearance.

The vast majority are at secret level and below, and there much less stringent procedures have been in place both for conducting investigations and for determination of who might have access.

In the current case, John Walker and Jerry Whitworth were in the category of those with access to top secret and crypto clearances. So simply reducing sharply the number of people cleared would not have impacted on their access.

Q: What about remedies?

A: One problem is the basic attitude of the society at large about selling secrets. It's a basic question of ethics. It impacts too on the sale of industrial secrets in corporations, but of course much more significantly on the damage done to the country at large from the sale of the government's secrets.

We're going to have to increase the penalties. I'm inclined at this point to mandatory life sentences without parole for those who have sold the country's secrets.

We need to find some way to create incentives for those who suspect that an individual is selling secrets to alert the authorities—and not wait years. I don't have any good answer what those incentives might be. They could range from being an accessory to the crime if they don't report it all the way on to pandering to the same greed that creates most of these cases in the first place—offering rewards for reporting if it leads to an arrest and a conviction.

What we don't want to do is to create a climate where there are all kinds of mindless allegations, and a person has a cloud over his head until he proves himself innocent.

On the question of what is classified, obviously the system could stand a good rigorous wirebrushing and an examining both of what is classified and of how many people need to have access to it. But my sense is that's not going to have a major effect. There clearly needs to be more resources applied to the job of screening individuals who have access.

In the area of personal security investigations, I believe we should consider substantially wider use of polygraph in the process of trying to get through clearance of a much larger group of people. Not polygraph to inquire into everybody's personal private life: after all, blackmail hasn't shown up as an element in any of these cases. But there are two fundamental areas that wouldn't take very long to look for some kind of difficulty.

One is financial status: does the person have unaccounted-for outside income? Is he living substantially beyond the means of the salary he's being paid or other financial arrangements that he's prepared to account for?

The second one is: does he have any kind of contact with individuals from other countries, or whom he believes may be acting on behalf of other countries, who have attempted to solicit classified information? Certainly as you look at this case, one of the early areas for these approaches would be those who handle communications, cryptographic equipment.

When one looks further out, there's clearly also an advantage to random rechecks. One of the great success stories of the last couple of years has been the program to drastically reduce drug use within the military. And its answer has been the urinalysis tests, officer and enlisted, and then the random re-analysis along the way. I believe the reasonable prospect that there would be unscheduled recurring checks of polygraph—all we'll need is two simple questions—could have a dramatic impact.